ITespresso.fr
La dose d'actu IT pour les TPE-PME
Connectez-vous
ABONNEZ-VOUS AUX NEWSLETTERS
SOLUTIONS IT | EQUIPEMENT IT | E-COMMERCE | FINANCEMENT IT | MARCHÉ IT | TÉLÉCHARGER | IT WEB TV
IT | Marketing | Achats | Commercial | Dirigeant | DAF | DRH | Cloud | Sécurité | Stockage | Mobilité | Livres Blancs | Quiz | Test débit | Evénement | Zones Partenaires | 4G

SÉCURITÉ WORDPRESS : ATTENTION À L'EXTENSION MAILPOET

Plus de 50 000 sites et blogs WordPress auraient déjà été ciblés à travers l'extension MailPoet, dont toutes les versions sorties avant le 3 juillet 2014 abritent une faille de sécurité.

Le 25 juillet 2014 par Clément Bohic 0 Commentaire Donnez votre avis

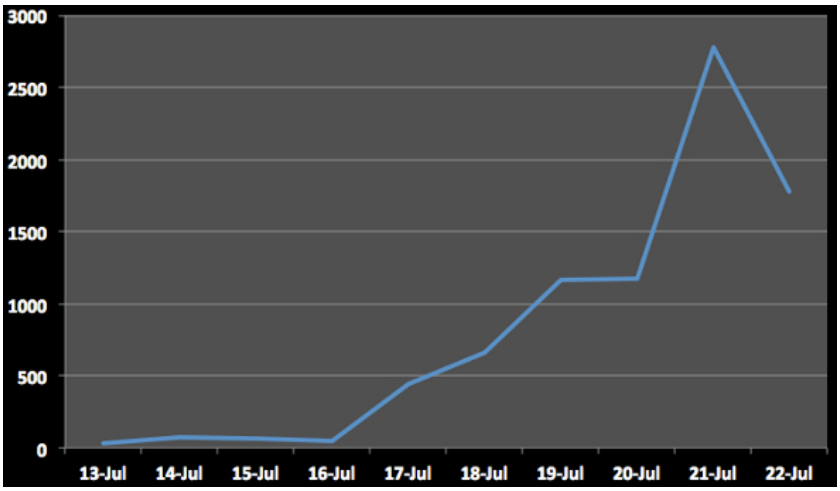
Depuis plusieurs semaines, **MailPoet** (ex-Wysija) est sous haute surveillance.

Destinée à mettre en place une newsletter sur les blogs et sites **WordPress**, cette extension a été téléchargée près de 2 millions de fois et bénéficie d'une note de 4,9/5 sur la base de plus d'un millier d'évaluations. Mais elle abrite une **faille de sécurité** qui permet de transférer n'importe quel fichier vers le serveur vulnérable, sans authentification. Des pirates peuvent l'utiliser pour héberger des logiciels malveillants, mais aussi à des fins de phishing ou d'envoi de spam.

Signalée à l'éditeur au mois de juin et corrigée dans la foulée, la faille a été rendue publique le 1er juillet. Problème : le message a du mal à passer. Sur son blog, l'éditeur de MailPoet précise clairement que seule la version 2.6.8 de son extension – sortie le 3 juillet – est sécurisée (bien qu'il existe un patch pour qui souhaiterait impérativement continuer à exploiter une mouture plus ancienne). Mais jour après jour, la situation ne semble pas s'améliorer : plus de 50 000 sites auraient été ciblés depuis le début des attaques, à en croire la firme de sécurité Sucuri.

Il est d'autant plus urgent de réagir que de nombreux thèmes WordPress intègrent MailPoet par défaut. En plus d'une mise à jour de l'extension sans délai pour tous les utilisateurs, une vérification et un nettoyage des sites est recommandé et pour cause : la porte dérobée ouverte par cette vulnérabilité donne aux pirates un contrôle total. Elle crée en l'occurrence un utilisateur « 1001001″ et lui donne les privilèges administrateurs… notamment pour écraser des fichiers, ce qui rend la restauration difficile si l'on n'a pas prévu de stratégie de backup.

Les entreprises touchées retrouvent généralement, dans chaque fichier PHP de leur site, du texte chiffré. Nombre d'entre elles s'aperçoivent que le serveur de diffusion PHP mailer a servi à envoyer des milliers de spams. Les symptômes varient, mais plusieurs victimes s'accordent sur un point : la nécessité de mettre en place un système d'alertes que les développeurs de modules pourraient faire remonter directement dans l'interface d'administration WordPress.



Les sites infectés se comptent par milliers (source Sucuri).

——A voir aussi ——
Quiz ITespresso.fr : que savez-vous des CMS open source ?

Crédit photo : FreshPaint – Shutterstock.com

Restez connectés, inscrivez-vous gratuitement à notre newsletter ! >>

Clément Bohic
Journaliste

SONDAGE
Dans les objets connectés, qu'est-ce qui vous séduit en premier ?
Le design
L'usage pratique
Revoir le quotidien avec des fonctions innovantes
Rien. Que du pipeau
Vote Voir les résultats

ITWEB TV : LA TÉLÉVISION IT

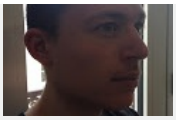
SUIVEZ-NOUS
Télécharger | Emploi
Twitter | Facebook
Google Currents | Google +
IOS Application | Android Application
Windows Phone | Flux RSS
Blackberry Application

TÉLÉCHARGEZ LES DERNIERS LOGICIELS
Convertisseur MP3
Xilisoft Convertisseur Vidéo
Facebook Toolbar Button
Mozilla Firefox
µTorrent

THÉMATIQUES IT
» Android
» Cloud
» Fibre
» Mobilité
» Steve Ballmer
» Jérémie Berrebi
» Eric Boustouller
» Tim Cook

Lire mes autres articles

Mon article vous a plu ?
Restez-connectés en vous inscrivant à nos newsletters



Suivez-moi

Google + Twitter Facebook Linkedin

» PME
» Réseau Social
» Smartphone
» Start-Up
» Stockage
» Tablette
» Virtualisation
» Windows
» Stephen Elop
» Jacques-Antoine Granjon
» Xavier Niel
» Marc Simoncini
» Stephane Richard
» Mark Zuckerberg

Autres articles sur ce sujet

Sécurité IT : un ver contamine les blogs

Sécurité IT : des thèmes gratuits pour

WordPress : une faille « zero-day »

WordPress 3.6.1 : la sécurité par le PHP

AVAST! ANTIVIRUS

Plus de 200 millions de personnes font confiance à avast! pour protéger leurs appareils - plus que tout autre antivirus Et il devient encore meilleur. Téléchargez- le maintenant !

LIVRES BLANCS ASSOCIÉS

Six éléments essentiels pour la sécurité des applications Web
23.07.2014, Qualys

Se prémunir des Zero Day dans la gestion des vulnérabilités
15.07.2014, Qualys

Les meilleures pratiques pour sélectionner une solution d'analyse des applications Web (WAS)
15.07.2014, Qualys

Sécurité et virtualisation - Conseils pratiques pour vous aider à protéger vos systèmes et données sensibles
20.06.2014, Kaspersky

Voir tous nos livres blancs ...

DERNIERS COMMENTAIRES

0 replies to *Sécurité WordPress : attention à l'extension MailPoet*

Laisser un commentaire

Les champs obligatoires sont indiqués avec *,
Votre adresse de messagerie ne sera pas publiée.

Nom*

E-Mail*

Site web

Commentaire

Vous pouvez utiliser ces balises et attributs HTML : <a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <strike>

Laisser un commentaire

Tags : CMS, e-mailing, mailpoet, Sécurité, Wordpress.

« Article précédent Article suivant »

ARTICLES RÉCENTS

Nokia Lumia 530 : un Windows Phone 8.1 pour moins de 100 euros

Marketing : Quantifind boucle un tour de table de 12 millions de dollars

Numérique : un premier « project bond » pour le très haut débit

ÉVÉNEMENTS

Salon e-Commerce
Du Mardi 23 septembre 2014 au Jeudi 25 septembre 2014

Les Assises de la Sécurité et des Services d'Information
Du Mercredi 01 octobre 2014 au Vendredi 03 octobre 2014

Mobility For Business 2014
Du Mercredi 15 octobre 2014 au Jeudi 16 octobre 2014
09:00 - 19:00

Europioneers Awards 2014
Le Lundi 03 novembre 2014

Voir tous les événements

RECHERCHE SOCIÉTÉ

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

E-commerce | Equipement IT | Financement IT | Marché IT | Solutions IT

Boris GOURMELEN : « Corporama aide ses clients à gagner en efficacité commerciale »
Le salon e-Commerce Paris 2014 ouvrira ses portes le 23 septembre
M-commerce : les applications et le responsive design sont délaissés
Chronodrive adopte Hiku et sa télécommande e-commerce
Vidéo Denis Caminade (Shops Agency) : Le poids (relatif) du digital à l'ère du full commerce

Articles suivants

Nokia Lumia 530 : un Windows Phone 8.1 pour moins de 100 euros
Sécurité IT : Apple capable d'espionner ses terminaux iOS ?
Mini-PC : la révolution est en marche
Fibre optique : Google intéressé par le Royaume-Uni
Le Chromecast de Google s'enrichit du mirroring

Articles suivants

Marketing : Quantifind boucle un tour de table de 12 millions de dollars
Financement : des signes positifs pour le crowdfunding
Le calendrier intelligent Sunrise lève 6 millions de dollars
Télécoms : Optiflows lève 400 000 euros
Gestion du risque client : XHI Solutions boucle un tour de table de 150 000 euros

Articles suivants

Numérique : un premier « project bond » pour le très haut débit
La diversité n'est pas le point fort de Twitter
Vidéo Gabriel Dabi-Schwebel (agence 1min30) : « Inbound Marketing : les clients viennent vers vous »
Résultats Amazon : l'innovation pèse sur les bénéfices
Droit à l'oubli : l'engrenage est lancé en Europe

Articles suivants

Google Maps Engine Pro : une dimension RH dans la cartographie

Sécurité WordPress : attention à l'extension MailPoet

Skype arrive sur le Fire Phone et Skype 5.0 prochainement pour Android

4G+ : Orange et Bouygues Telecom livrent bataille en coulisse

EasyJet teste la technologie iBeacon dans les aéroports

Articles suivants